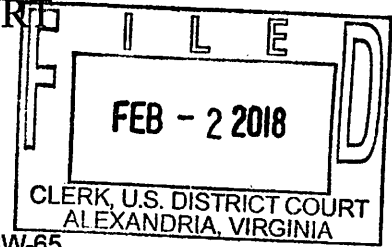


UNITED STATES DISTRICT COURT

for the
Eastern District of VirginiaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)THE CELLULAR TELEPHONE ASSIGNED CALL
NUMBER 703-269-7719

Case No. 1:18-SW-65

1:18-EC-189

UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A: This Court has authority to issue this Warrant under 18 U.S.C. §§ 2703(c)(1)(A) and 2711(3)(A) and Federal Rule of Criminal Procedure 41.

located in the _____ District of New Jersey, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☐ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1344 and 1349	Conspiracy to Commit Bank Fraud

The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.
☒ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA:
Alexander P. Berrang

Applicant's signature

Gregory Settducati, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 2/2/18

_____/s/
 Michael S. Nachmanoff
 United States Magistrate Judge

Judge's signature

City and state: Alexandria, Virginia

The Honorable Michael S. Nachmanoff, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

Property to Be Searched

1. The cellular telephone assigned call number **(703) 269-7719** (hereinafter, the **"TARGET CELL PHONE"**), whose wireless service provider is T-Mobile US, Inc., a company that is headquartered in Bellevue, Washington and that accepts service of legal process via its Custodian of Records with its Law Enforcement Relations Team located at 4 Sylvan Way, Parsippany, NJ 07054.

2. Information about the location of the **TARGET CELL PHONE** that is within the possession, custody, or control of T-Mobile.

ATTACHMENT B

Particular Things to be Seized

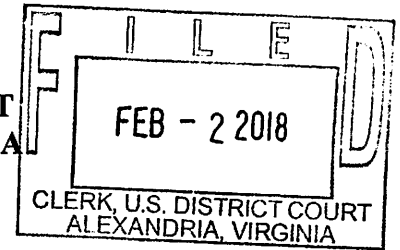
All information about the location of the **TARGET CELL PHONE** described in Attachment A for a period of thirty days, during all times of day and night. “Information about the location of the **TARGET CELL PHONE**” includes all available T-Mobile, GPS data, latitude-longitude data, and other precise location information, as well as all data about which “cell towers” (*i.e.*, antenna towers covering specific geographic areas) and “sectors” (*i.e.*, faces of the towers) received a radio signal from the cellular telephone described in Attachment A.

To the extent that the information described in the previous paragraph (hereinafter, “Location Information”) is within the possession, custody, or control of T-Mobile, T-Mobile is required to disclose the Location Information to the government. In addition, T-Mobile must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with T-Mobile’s services, including by initiating a signal to determine the location of the **TARGET CELL PHONE** on T-Mobile’s network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate T-Mobile for reasonable expenses incurred in furnishing such facilities or assistance.

This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF
THE CELLULAR TELEPHONE ASSIGNED
CALL NUMBER 703-269-7719

Case No. 1:18-sw-65
1:18-ec-189

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Gregory R. Settducati, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A) for information about the location of a cellular telephone assigned call number (703) 269-7719 (hereinafter, "**TARGET CELL PHONE**"). The service provider for **TARGET CELL PHONE** is T-Mobile US Inc. ("T-Mobile"), a wireless telephone service provider headquartered in Bellevue, Washington, that accepts legal service via the Custodian of Records with its Law Enforcement Relations Team located at 4 Sylvan Way, Parsippany, New Jersey 07054. The **TARGET CELL PHONE** is described herein and in Attachment A, and the location of the information to be seized is described herein and in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been since February 2012. I am currently assigned to a squad which investigates organized crime and criminal enterprises out of the Washington Field Office, Northern Virginia Resident Agency. My duties with the FBI include, but are not limited to, the investigation of criminal enterprises and alleged violations of federal criminal statutes, including bank, mail, and wire fraud, money

laundering, and crimes which involve financial institutions. I have conducted physical and electronic surveillance, executed search and arrest warrants, and reviewed and analyzed records and documents for fraudulent activity. I have interviewed suspects, defendants, witnesses, victims, and spoken to other experienced investigators concerning the methods and practices of criminal enterprises. In addition, I am a graduate of the FBI Academy, and have received training in cyber security matters.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1344 and 1349 (Conspiracy to Commit Bank Fraud) have been committed by **SIRANUSH YENGIBARYAN** and **RADIK KARAPETYAN**. On or about January 25, 2018, **YENGIBARYAN** and **KARAPETYAN** were charged by complaint in the Eastern District of Virginia with this crime and now are the subjects of arrest warrants. Accordingly, there is probable cause to believe that the location information described in Attachment B will assist law enforcement in arresting **YENGIBARYAN**, who is considered a “person to be arrested” within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

PROBABLE CAUSE

A. Overview of the Conspiracy Under Investigation

5. As described further below, on numerous occasions, **KARAPETYAN** and **YENGIBARYAN** have fraudulently obtained money from Automated Teller Machines (“ATMs”) and U.S. Postal Service (“USPS”) points-of-sale by utilizing physical cards encoded

with payment card numbers (*i.e.*, credit or debit card numbers) that they were not authorized to possess or use. I know that the conspiracy described herein has victimized a number of financial institutions, and I know that, at the time of the criminal conduct, at least the following financial institutions were insured by the Federal Deposit Insurance Corporation: Bank of America; BB&T; and Capital One Bank.

6. There is reason to believe—based on my training, experience, and the information learned through this investigation—that the payment card numbers utilized by **KARAPETYAN** and **YENGIBARYAN** initially were obtained via skimming devices, or “skimmers,” which are computer hardware that can be installed within legitimate electronic payment mechanisms in order to capture and misappropriate payment card information. This is so for at least the following reasons.

7. *First*, as explained below, **YENGIBARYAN**’s unauthorized use of at least one of the misappropriated payment card numbers was preceded by the authorized account holder’s use of that payment card number at a gas station in northern Virginia. In my training and experience, criminals engaged in skimming frequently target gas pumps because the electronic payment systems attached to these pumps are not as well monitored as systems attached to traditional cash registers. I also know that such criminals usually attach skimmers to the electronic components of gas pumps that accept customers’ payment cards and read those cards in order to render payment for the purchased gasoline.

8. *Second*, I know from my training and experience that withdrawing money from ATMs generally requires the entry of a personal identification number, of “PIN.” Because **KARAPETYAN** and **YENGIBARYAN** successfully withdrew money from ATMs with misappropriated payment card numbers, it is reasonable to believe that they knew the PINs

associated with those numbers. I know from my training and experience that it is possible for skimmers to electronically capture, among other data, PINs from cards that are swiped through the devices.

9. *Third*, the fraudulent transactions in which **KARAPETYAN** and **YENGIBARYAN** engaged are indicative of individuals involved in skimming. In my training and experience, once payment card numbers are misappropriated via a skimmer, frequently the next step is to conduct “cash-outs,” *i.e.*, to use the misappropriated payment cards to make unauthorized withdrawals from ATMs and conduct fraudulent purchases. In order to conduct cash-outs, criminals typically encode the stolen payment card numbers onto physical cards. The encoding process typically requires a computer and a magnetic strip reader with rewriting capability, and criminals have been known to re-encode the magnetic strips of calling cards, debit cards, or credit cards with misappropriated payment card numbers. The re-encoded cards then are used to make ATM withdrawals and/or to purchase money orders from the USPS. In my training and experience, USPS money orders are purchased because they work like cash and generally have higher maximum purchases than one could withdraw from an ATM (*e.g.*, the purchase limit for postal money orders is \$3,000, whereas ATM withdrawal limits are typically between \$400 and \$600).

B. YENGIBARYAN’s Involvement in the Conspiracy

10. As described below, it appears from the investigation that **YENGIBARYAN** has defrauded multiple financial institutions through a series of ATM-related and USPS-related transactions. I am familiar with **YENGIBARYAN**’s appearance through my review of known photographs of her.

Fraudulent Cash Withdrawals from ATMs

11. A review of records provided by various banks (including account records and surveillance images) reveals that between on or about May 15, 2017, and June 27, 2017, a woman who appears to be **YENGIBARYAN** used, without authorization, at least three payment card numbers to make at least six withdrawals of money from Bank of America and BB&T ATMs that totaled approximately \$1,780. These transactions are set forth in the table below.

Approximate Date & Time	Location of Activity	Withdrawal
May 15, 2017, at 20:43	Bank of America ATM (IMDN2051) 7370 Baltimore Ave. College Park, MD 20740	\$300.00 withdrawal via State Department Federal Credit Union card ending in 8332.
June 22, 2017, at 09:09	BB&T ATM (A876) 380 Main Street Laurel, MD 20707	\$500.00 withdrawal via Bank of America card ending in 5453.
June 23, 2017, at 10:55	BB&T ATM (A876) 380 Main Street Laurel, MD 20707	\$320.00 withdrawal via Bank of America card ending in 5453.
June 23, 2017, at 10:56	BB&T ATM (A876) 380 Main Street Laurel, MD 20707	\$60.00 withdrawal via Bank of America card ending in 5453.
June 23, 2017, at 10:57	BB&T ATM (A876) 380 Main Street Laurel, MD 20707	\$100.00 withdrawal via Bank of America card ending in 5453.
June 27, 2017, at 12:22	BB&T ATM (A719) 1097 Seven Locks Road Rockville, MD 20854	\$500.00 withdrawal via Bank of America card in 0439.

12. According to records obtained from the State Department Federal Credit Union and Bank of America, the accounts ending in 8332, 5453, and 0439 respectively belonged to real persons who will be identified herein as P.J., M.P., and C.K. HSI also has determined through its investigation that **YENGIBARYAN** made the withdrawals described above without the

authorization of the State Department Federal Credit Union, Bank of America, or the legitimate account holders of the payment card numbers.

13. It appears that at least one of the payment card numbers discussed above was obtained via a skimming incident at a gas station in northern Virginia. The reason for this belief is that, according to information provided by Capital One, on or about June 21, 2017, M.P. used the payment card number ending in 5453 to purchase fuel at a gas station located in McLean, Virginia, which is within the Eastern District of Virginia, and it was subsequent to that purchase that M.P.'s card was used to make the four ATM withdrawals identified above, as well as four, unauthorized USPS purchases.

Fraudulent USPS Money Order Purchases, Deposits, and Cash Outs

14. In addition, through its investigation, law enforcement officers with USPS have determined that **YENGIBARYAN** has cashed multiple USPS money orders and deposited multiple USPS money orders into a Citibank account ending in 1633 via Citibank branches in California and Maryland locations. (Records from Citibank indicate that the account ending in 1633 is jointly owned or controlled by **YENGIBARYAN** and her husband.)

15. Specifically, a review of surveillance images and related records provided by Citibank indicates that between on or about May 24, 2017, and on or about August 10, 2017, a woman who appears to be **YENGIBARYAN** cashed approximately 31 USPS money orders totaling approximately \$16,798 and deposited approximately 13 USPS money orders totaling \$7,750, as detailed in the table below:

Approximate Date & Time	Number of USPS Money Orders	Total Amount Deposited or Cashed
May 24, 2017	4	Cashed \$2,700.00
May 30, 2017	10	Cashed \$3,150.00
June 2, 2017	9	Cashed \$5,500.00

Approximate Date & Time	Number of USPS Money Orders	Total Amount Deposited or Cashed
June 26, 2017	3	Deposited \$1,950.00 into Citibank account ending 1633
June 27, 2017	3	Deposited \$1,700.00 into Citibank account ending 1633
June 30, 2017	2	Deposited \$1,100.00 into Citibank account ending 1633
July 5, 2017	4	Cashed \$2,688.00
Aug. 8, 2017 (at 11:45 hrs.)	5	Deposited \$3,000.00 into Citibank account ending 1633
Aug. 8, 2017 (at 13:18 hrs.)	4	Cashed \$2,760.00

It should be noted that surveillance footage associated with the cashing of the USPS money orders on or about May 24, 2017, depict a woman who appears to be **YENGIBARYAN** at a Citibank branch in North Hollywood, California, with a male who appears to be **KARAPETYAN**. The video appears to show **YENGIBARYAN** endorsing what appear to be USPS money orders, cashing them for U.S. currency, and then handing the U.S. currency to **KARAPETYAN**, who appears to be assisting her with the transaction.

16. By reviewing each USPS money order deposited or cashed by **YENGIBARYAN**, USPS agents were able to identify each money order's serial number and Post Office finance numbers. USPS agents then entered these numbers into a USPS database, and determined the payment card number that was used to purchase each USPS money order, as well as the location of the purchase. Listed in the table below are those USPS money order transactions that, based on a review of bank records, were determined to have been purchased fraudulently:

Date Purchased	Serial Number	Location of Money Order Purchase	Payment Card Used	Date Deposited
May 16, 2017	24566554888	U.S. Post Office 3709 Rhode Island, Ave. Mount Rainer, MD	M&T Bank card ending in 1655	May 24, 2017

Date Purchased	Serial Number	Location of Money Order Purchase	Payment Card Used	Date Deposited
May 17, 2017	24056698443	U.S. Post Office 12975 Highland Rd. Highland, MD	Apple Federal Credit Union card ending in 0452	June 2, 2017
June 22, 2017	2399169451	U.S. Post Office 3375 Ellicott Center Dr. Ellicott City, MD	Navy Federal Credit Union card ending in 9898	June 26, 2017
June 22, 2017	24497824127	U.S. Post Office 2513 North Rollins Rd. Windsor Mill, MD	Navy Federal Credit Union card ending in 9898	June 26, 2017
June 23, 2017	24195245095	U.S. Post Office 143 Rolling Rock Ave. Rockville, MD	M&T Bank card ending in 6387	Aug. 8, 2017
June 24, 2017	23920774637	U.S. Post Office 111 Washington Grove Ln. Washington Grove, MD	InTouch Credit Union card ending in 4978	June 27, 2017
June 24, 2017	23920774626	U.S. Post Office 111 Washington Grove Ln. Washington Grove, MD	InTouch Credit Union card ending in 4978	June 27, 2017
June 26, 2017	24581256704	U.S. Post Office 6655 Santa Barbara Rd. Elkridge, MD	Bank of America card ending in 3532	Aug. 8, 2017
June 27, 2017	24082988433	U.S. Post Office 16501 Shady Grove Rd. Gaithersburg, MD	Sandy Spring Bank card ending in 3241	Aug. 9, 2017
June 27, 2017	24082988400	U.S. Post Office 16501 Shady Grove Rd. Gaithersburg, MD	Bank of America card ending in 8089	Aug. 10, 2017
June 29, 2017	24031807863	U.S. Post Office 4001 Buckeystown Pike, Buckeystown, MD	Sun Trust Bank card ending in 7065	June 30, 2017
June 29, 2017	23938087950	U.S. Post Office 12774 Wisteria Dr. Germantown, MD	SunTrust Bank card ending in 2306	July 5, 2017

Date Purchased	Serial Number	Location of Money Order Purchase	Payment Card Used	Date Deposited
June 29, 2017	24082988692	U.S. Post Office 16501 Shady Grove Road, Gaithersburg, MD	Bank of America card ending in 4869	Aug. 8, 2017
June 30, 2017	24082988804	U.S. Post Office 16501 Shady Grove Rd. Gaithersburg, MD	BB&T Bank card ending in 4093	Aug. 8, 2017

17. A review of the money orders listed above indicates that a number of the money orders were endorsed with **YENGIBARYAN**'s name prior to them being deposited. The serial numbers of those money orders were as follows: No. 24497824127; No. 23920774637; No. 23920774626; No. 241952545095; No. 24082988692; No. 24082988804; and No. 24581256704.

18. Based on records received from the financial institutions listed in the table above, all of the payment card numbers identified in the table above had been issued to real persons other than **YENGIBARYAN** or **KARAPETYAN**, and neither **YENGIBARYAN** nor **KARAPETYAN** had been authorized by the financial institution that had issued the payment card number or the person who owned or controlled the payment card number to make any transactions.

C. KARAPETYAN's Involvement in the Conspiracy

19. A review of records provided by BB&T and Capital One (including account records and surveillance images) reveals that between on or about August 23, 2017, and December 27, 2017, a man used, without authorization, at least seven payment card numbers to make (or attempt to make) at least eight withdrawals of money from BB&T ATMs located in Vienna, Virginia, which is within the Eastern District of Virginia, and Columbia, Maryland. I have reviewed known photographs of **KARAPETYAN** and am familiar with his appearance,

and it is my determination that **KARAPETYAN** is the man seen engaging in the aforementioned transactions. These transactions are set forth in the table below.

Approximate Date & Time	Location of Activity	Attempted and/or Withdrawals
Aug. 23, 2017, at 17:51	BB&T ATM (AE02) 8385 Leesburg Pike A Vienna, VA 22182	\$500.00 attempted withdrawal via Capital One Bank card ending in 0786.
Aug. 23, 2017, at 17:54	BB&T ATM (AE02) 8385 Leesburg Pike A Vienna, VA 22182	\$500.00 attempted withdrawal via Capital One Bank card ending in 3735.
Dec. 27, 2017, at 02:20	BB&T ATM (AR06) 8801 Columbia 100 Parkway Columbia, MD 21045	\$300.00 withdrawal via Capital One Bank card ending in 4866.
Dec. 27, 2017, at 02:20	BB&T ATM (AR06) 8801 Columbia 100 Parkway Columbia, MD 21045	\$60.00 withdrawal via Capital One Bank card ending in 4866.
Dec. 27, 2017, at 02:24	BB&T ATM (AR06) 8801 Columbia 100 Parkway Columbia, MD 21045	\$100.00 attempted withdrawal via Capital One Bank card ending in 5444.
Dec. 27, 2017, at 02:26	BB&T ATM (AR06) 8801 Columbia 100 Parkway Columbia, MD 21045	\$60.00 attempted withdrawal via Capital One Bank card ending in 6680.
Dec. 27, 2017, at 02:26	BB&T ATM (AR06) 8801 Columbia 100 Parkway Columbia, MD 21045	\$60.00 attempted withdrawal via Capital One Bank card ending in 1507.
Dec. 27, 2017, at 02:28	BB&T ATM (AR06) 8801 Columbia 100 Parkway Columbia, MD 21045	\$300.00 attempted withdrawal via Capital One Bank card ending in 7335.

It should be noted that the December 27, 2017 transactions identified in the table above were conducted via a drive-up ATM. Surveillance footage from that ATM depict a man who appears to be **KARAPETYAN** in the driver's seat conducting the transactions, an unknown male in the

front passenger seat, and a woman who appears to be **YENGIBARYAN** in one of the back seats of the vehicle.

20. According to records obtained from Capital One Bank, the accounts ending in 0786, 3735, 4866, 5544, 6680, and 7335 respectively belonged to real persons who will be identified herein as R.S., Y.H., J.C., A.B., D.D., and D.P. HSI also has determined through its investigation that **KARAPETYAN** made the withdrawals described above without the authorization of the Capital One or the legitimate account holders of the payment card numbers.

D. Additional Connections between YENGIBARYAN and KARAPETYAN

21. The investigation to date has provide at least three additional reasons to believe that **YENGIBARYAN** and **KARAPETYAN** have joined together to further the conspiracy described herein.

22. *First*, records obtained from Enterprise Rent-A-Car indicate that on or about June 23, 2017, at approximately 10:47 a.m., a red 2017 Nissan Rogue bearing Maryland license plate 3CY0498 was rented from an Enterprise location in Laurel, Maryland. The vehicle was rented in **YENGIBARYAN**'s name and a California driver's license in **YENBIARYAN**'s name was presented at the time of the rental. Enterprise's records further show that, initially, a payment card ending in 6728 was presented for payment, but was declined. Thereafter, a payment card ending in 9135 and in **KARAPETYAN**'s name was used to secure the rental. On or about June 25, 2017, BB&T Bank ATM surveillance captured this Nissan Rogue at a BB&T ATM in Elkridge, Maryland, withdrawing money, and on or about June 26, 2017, at approximately 10:21 a.m., the vehicle was returned to Enterprise after having been driven approximately 267 miles.

23. *Second*, on or about September 7, 2017, law enforcement officers with the Drug Enforcement Agency ("DEA") were conducting passenger screenings at the Detroit Metropolitan

Airport when they encountered **YENGIBARYAN** and **KARAPETYAN** at Gate A-24 in the McNamara Terminal. **YENGIBARYAN** and **KARAPETYAN** each had a ticket for Delta Airlines flight 1906, which was destined for Los Angeles, California. **KARAPETYAN** identified **YENGIBARYAN** as his cousin and stated to DEA law enforcement officers that they were traveling together through Baltimore to New York for vacation. **KARAPETYAN** also stated that he was only traveling with \$2,000; however, after a consensual search, DEA law enforcement discovered \$12,465.00 in U.S. currency on **KARAPETYAN**'s person. This money subsequently was seized by DEA law enforcement officers.

24. With the consent of **YENGIBARYAN** and **KARAPETYAN**, DEA officers searched their luggage. DEA officers thereafter found seven USPS money orders totaling \$3,550 in **YENGIBARYAN**'s luggage. Law enforcement officers discovered that all the USPS money orders were purchased with compromised payment cards and the transactions were reported as fraudulent based on bank records.

25. The DEA officers also seized from **YENGIBARYAN**'s carry-on luggage a total of \$18,230 in U.S. currency and two California driver's licenses. Although both licenses included a picture of **YENGIBARYAN**, one of the licenses was in the name of an individual identified herein as C.S. and the other was in the name of an individual identified herein as M.C. HSI has determined that C.S. and M.C. are real persons who reside in California. Notably, the licenses found within **YENGIBARYAN**'s luggage listed addresses, dates of birth, and license numbers that, based on a records check by HSI, matched the respective addresses, dates of birth, and license numbers of C.S. and M.C. Moreover, a review of records from the California Department of Motor Vehicles shows that **YENGIBARYAN** has a California driver's license under her own name and with her photograph.

26. *Third*, on or about November 8, 2017, a representative of Hyatt House in Gaithersburg, Maryland, met with law enforcement and advised that **YENGIBARYAN** reserved rooms in her name for October 28, 2017 through November 2, 2017, and on November 6, 2017 to November 7, 2017. The Hyatt House representative also was shown a photo array containing 11 photographs of individuals—two of which were known photographs of **YENGIBARYAN** and **KARPETYAN**—and identified **YENGIBARYAN** and **KARPETYAN** as both being at the Hyatt House within the last few days.

E. THE TARGET CELL PHONE

27. It appears from the investigation that **YENGIBARYAN** currently uses **TARGET CELL PHONE**. The bases for this conclusion is that law enforcement has determined that **TARGET CELL PHONE** was associated with a January 2018 hotel reservation in the name of **YENGIBARYAN**. Additionally, on or about January 26, 2018, law enforcement identified a publically accessible Facebook account in the name of **SIRANUSH YENGIBARYAN**. A review of this public profile indicates that **TARGET CELL PHONE** is associated with that account.

28. In my training and experience, I have learned that T-Mobile is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate at least two kinds of information about the locations of the cellular telephones to which they provide service: (1) E-911 Phase II data, also known as GPS data or latitude-longitude data, and (2) cell-site data, also known as “tower/face information” or cell tower/sector records. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device’s signal using data

from several of the provider's cell towers. Cell-site data identifies the "cell towers" (*i.e.*, antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (*i.e.*, faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise than E-911 Phase II data.

29. Based on my training and experience, I know that T-Mobile can collect E-911 Phase II data about the location of the **TARGET CELL PHONE**, including by initiating a signal to determine the location of **TARGET CELL PHONE** on T-Mobile's network or with such other reference points as may be reasonably available.

30. Accordingly, based on my training and experience, I know that T-Mobile can collect cell-site data about the **TARGET CELL PHONE**. It is reasonable to believe that obtaining this information for a period of 30 days will assist law enforcement in arresting **YENGIBARYAN** due to her travel throughout the United States. Specifically, it appears from the investigation that **YENGIBARYAN** has travelled from California to the Washington, D.C. area on multiple occasions. Moreover, efforts to date to locate **YENGIBARYAN** have been met with negative results. It is reasonable to believe that **YENGIBARYAN** travels with the **TARGET CELL PHONE** because: (a) **YENGIBARYAN** has been observed with a cell phone during the course of the investigation; and (b) in my training and experience, cell phone users usually take their phones with them when they travel. Therefore, by collecting cell-site data about the **TARGET CELL PHONE** for a period of 30 days investigators will be able to locate and arrest **YENGIBARYAN**.

AUTHORIZATION REQUEST

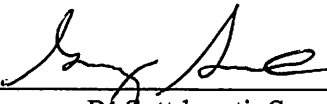
31. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c).

32. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of **TARGET CELL PHONE** would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).


33. I further request that the Court direct T-Mobile to disclose to the government any information described in Attachment B that is within the possession, custody, or control of T-Mobile. I also request that the Court direct T-Mobile to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with T-Mobile's services, including by initiating a signal to determine the location of **TARGET CELL PHONE**

on T-Mobile's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate T-Mobile for reasonable expenses incurred in furnishing such facilities or assistance.

Respectfully submitted,



Gregory R. Settducati, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on this 2nd day of February, 2018:
_____/s/ 
Michael S. Nachmanoff
~~United States Magistrate Judge~~
The Honorable Michael S. Nachmanoff
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

1. The cellular telephone assigned call number **(703) 269-7719** (hereinafter, the **“TARGET CELL PHONE”**), whose wireless service provider is T-Mobile US, Inc., a company that is headquartered in Bellevue, Washington and that accepts service of legal process via its Custodian of Records with its Law Enforcement Relations Team located at 4 Sylvan Way, Parsippany, NJ 07054.

2. Information about the location of the **TARGET CELL PHONE** that is within the possession, custody, or control of T-Mobile.

ATTACHMENT B

Particular Things to be Seized

All information about the location of the **TARGET CELL PHONE** described in Attachment A for a period of thirty days, during all times of day and night. “Information about the location of the **TARGET CELL PHONE**” includes all available T-Mobile, GPS data, latitude-longitude data, and other precise location information, as well as all data about which “cell towers” (*i.e.*, antenna towers covering specific geographic areas) and “sectors” (*i.e.*, faces of the towers) received a radio signal from the cellular telephone described in Attachment A.

To the extent that the information described in the previous paragraph (hereinafter, “Location Information”) is within the possession, custody, or control of T-Mobile, T-Mobile is required to disclose the Location Information to the government. In addition, T-Mobile must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with T-Mobile’s services, including by initiating a signal to determine the location of the **TARGET CELL PHONE** on T-Mobile’s network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate T-Mobile for reasonable expenses incurred in furnishing such facilities or assistance.

This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).